8 Best Practices for Working Remotely

Alex Laws

Analyst

Back to the News Desk

Companies of all sizes are under attack. Meanwhile, remote work has become a necessity for modern organizations looking to recruit talent and create business continuity plans. A good example of business continuity occurred in the spring of 2020, when organizations around the world sent hundreds of thousands of information workers to work from their home offices in response to the COVID19 (coronavirus) outbreak.

Remote work presents a unique challenge for information security because remote work environments don't usually have the same safeguards as in the office. When an employee is at the office, they are working behind layers of preventive security controls. While not perfect, it is harder to make a security mistake while at the office. However, when computers leave the perimeter and people work remote, new risks arise for the company and additional security policies are essential.

Here are some of the policy guidelines we suggest when you or your employees are outside the office:

Digital Security While Working Remotely

1. **Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection.**
   Public Wi-Fi introduces significant security risk and should be avoided if possible. If you need to access the internet from a public Wi-Fi location, you have two essential problems to solve. First, other people have access to that network and, without a firewall between you and them, threat actors can pound away at your computer from across the room. Second, any interested observers on either the current network or any other public networks your data hits between you and your workplace can monitor your traffic as it goes by. It is important to find a way to protect your PC and encrypt your traffic.

   One good option is to use a personal hotspot from a dedicated device or your phone. Although your web traffic will be unencrypted between the hotspot and its destination, using a hot spot does eliminate the problem of getting hacked by people on the same public Wi-Fi. With most major carriers, you can pay a nominal fee for the capability to set up a private Wi-Fi network with your cell phone. Of course, it will count against your data, but the cost is minimal relative to the potential downside of a significant hack to your company's systems or computer. If your company provides cell service, there's no reason not to use the hot spot to avoid public Wi-Fi especially given that, in many cities, 4G or 5G service is almost as fast as your home network access.

   For many remote access applications, you should use a VPN. VPNs provide a flexible connection to connect to different services (web pages, email, a SQL server, etc.) and can protect your traffic. Keep in mind that not all VPNs are worth the money; it's a good idea to evaluate your must-haves before you choose a VPN technology. Keep in mind that VPN services provided

for privacy purposes only protect the data to and from the VPN provider, not to the destination so are not suitable for protecting remote access.

Lastly, for some use cases, you can also set up encrypted remote connections into a remote desktop or other individual server. Many of these connection types (RDP, HTTPS, SSH) include encryption as part of their service direction and do not require an additional VPN or other encryption service to secure the data in-transit.

2. **Keep Work Data on Work Computers.**
   Thinking about taking care of a few emails at home before bed? If you take precautions like using your work computer, secure Wi-Fi, a VPN, encrypted drives, anti-virus, and endpoint protection, this may be totally fine. With that said, it can be tempting to use your personal computer if your work computer is in a different room or you forgot your charger at the office. This is a risk for you and for the company!

   If you work at an organization with an efficient IT team, they may be installing regular updates, running antivirus scans, blocking malicious sites, etc., and these activities may be transparent to you. There is a good chance you have not followed the same protocols with your personal computer as are mandatory at work. Furthermore, your company can likely afford higher end technical controls that you can personally. Without those running in the background, your personal computer is not safe for work information because it could be compromised by a third party. Essentially, by introducing a personal computer to a work network, even remotely, you've put the company networks at risk, and yourself at risk, accepting the potential liability of extensive corporate damages though violations of policy, practices or both.

   If your employer gives you access to a portal or remote access environment such as Office 365, you can work online and avoid downloading or synching files or emails to a personal device. It's always a best practice to keep personal business on personal technology, and only use your work-issued laptop for work-related business. In fact, many companies have stopped the "diminimus use" policy that allows employees to conduct personal business on work-owned assets in order to lower security risks.

3. **Block the Sight Lines.**
   If you are at a coffee shop, pay attention to your sight lines. If someone is behind you, they can see everything you are typing. Furthermore, someone with the right observational skills (like a cybercriminal) could easily watch what you are doing and identify confidential information. And keep your devices with you; in the time it takes you to use a restroom, your device could be quickly compromised by a threat actor with a USB stick that types pre-programmed sequences at 1000 words per minute. On a personal level, this is something you should do while keying in your ATM PIN as well.

4. **Encrypt Sensitive Data in Emails and on Your Device.**
   Sending emails with sensitive data is always going to be a risk. It could be intercepted or seen by

a third party. If you encrypt the data attached to an email, it will prevent an unintended recipient from viewing the information. Also, be sure your device is set to have all stored data encrypted in the case of theft.

Physical Security While Working Remotely

1. **Lock Your Doors.**
   This is Security 101: if you bring your work computer home or tend to work remotely, confidential corporate information could be at risk. When you get in the habit of always locking your doors, you have taken a key step toward improving your home office's security. A friend once had his work computer stolen from his 3rd floor walkup when he didn't lock the door! Don't subject yourself to the stress of a stolen work computer or harm your company by letting its data out into the wild.

   In heavily regulated industries, like healthcare, losing specific data could result in huge fines. Make sure these devices are encrypted in order to turn a disaster (data compromise) to an annoyance (loss of the device, but no compromise.) In many states, breach disclosure laws do not come into effect if the data was encrypted.

2. **Never Leave Your Devices or Laptop in the Car.**
   We advise our clients and employees to never leave their work computers or devices in a vehicle. It's a best practice to keep work laptops and devices on your person at all times while on the road. And the trunk of your car is not any safer. There may be criminals watching the parking lot from afar, waiting for their next victim. Putting valuables in the trunk may make life a little bit easier in the short-term - but why take that chance?

3. **Don't Use Random Thumb Drives.**
   A classic hacking technique is to drop a number of large capacity thumb drives near the company you are hoping to attack. The chances that an unwitting employee will pick up the thumb drive and use it are surprisingly high. Anecdotally, one of our employees ran a test on this at a previous job and a shocking percentage of people actually opened the files on the drive. If you are a hacker, BINGO - that's payday.

   Never use a thumb drive if you don't know where it came from and do not continue to use one if you have plugged it into a system for whose safety you cannot honestly vouch.

4. **Use a USB Data Blocker when Charging Up at a Public Phone Charging Station.**
   If you need to charge your phone and the only option is an unknown USB port, a wise measure is to protect it with a USB data blocker to prevent data exchange and guard against malware. This type of USB protection allows the device to connect to power without exposing the data pins inside your device; it connects the power leads, but not the data ones.